

2827

1FW

Docket No.: 2004P00922

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450.

By:

Date: August 30, 2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applic. No. : 10/592,018 Confirmation No: 7000
Applicant : Andreas Franke et al.
Filed : September 7, 2006
Art Unit : 2827
Title : Manipulation Proof Production of Authentic Random Numbers
Docket No. : 2004P00922
Customer No. : 24131

CLAIM FOR PRIORITY

Hon. Commissioner for Patents,
Alexandria, VA 22313-1450
Sir:

Claim is hereby made for a right of priority under Title 35, U.S. Code, Section 119, based upon the German Patent Application 10 2004 011 170.7 filed March 8, 2004.

A certified copy of the above-mentioned foreign patent application is being submitted herewith.

Respectfully submitted,

LAURENCE A. GREENBERG
REG. NO. 29,308

Date: August 30, 2007

Lerner Greenberg Sterner LLP
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: 954.925.1100
Fax: 954.925.1101

/mjb

BUNDESREPUBLIK DEUTSCHLAND



Prioritätsbescheinigung DE 10 2004 011 170.7 über die Einreichung einer Patentanmeldung

Aktenzeichen: 10 2004 011 170.7

Anmeldetag: 08. März 2004

Anmelder/Inhaber: Siemens Aktiengesellschaft,
80333 München/DE

Bezeichnung: Manipulationssichere Erzeugung
von echten Zufallszahlen

IPC: H 03 K 3/84, G 07 C 15/00

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der Teile der am 08. März 2004 eingereichten Unterlagen dieser Patentanmeldung unabhängig von gegebenenfalls durch das Kopierverfahren bedingten Farbabweichungen.

München, den 22. August 2007
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag


Werner

Beschreibung

Manipulationssichere Erzeugung von echten Zufallszahlen

- 5 Die vorliegende Erfindung betrifft ein Verfahren und eine Vorrichtung zur Erzeugung einer echten Zufallszahl.

Beispielsweise für Zugriffsschutz- oder Verschlüsselungszwecke ist es erforderlich, gute manipulationssichere Zufalls-
10 zahlen zu erzeugen. Im Zusammenhang mit Kraftfahrzeugwegfahrsperrern erfolgt diese Erzeugung der Zufallszahlen beispielsweise auf der Ebene der Motorsteuerung, bei der es sich in vielen Fällen um ein Embedded-System handelt. Dabei scheidet der Einsatz von externen Quellen aufgrund von Manipulations-
15 möglichkeiten und die Verwendung von speziellen Schaltkreisen wegen der damit verbundenen zusätzlichen Stückkosten aus.

Zur Erzeugung echter Zufallszahlen ist es unter anderem bekannt, die niederwertigen Bits einer A/D-Wandlung von Signalen einer separaten Rauschquelle zu verwenden, was jedoch mit
20 erheblichen Kosten verbunden ist. Es ist ebenfalls bekannt, eine echte Zufallszahl über eine Zeitmessung eines externen Ereignisses, beispielsweise der Dauer eines vom Benutzer vorgenommenen Tastendruckes, zu erzeugen. Diese Lösung scheidet
25 jedoch zumindest in den Fällen aus, in denen das System die Kommunikation eröffnet und daher vor einem externen Ereignis die Zufallszahl erzeugen muss. Neben der Erzeugung von echten Zufallszahlen ist es weiterhin bekannt, eine Pseudo-Zufallszahlenreihe zu nutzen und den aktuellen Status beispielsweise
30 in einem nicht-flüchtigen Speicher des Systems zu speichern. Allerdings ist die Qualität von Pseudo-Zufallszahlen im Vergleich zu echten Zufallszahlen unzureichend.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren sowie eine Vorrichtung anzugeben, mit denen eine echte Zufallszahl schnell, das heißt beispielsweise im Millisekundenbereich, speichersparend, geräteaufzeitunabhängig, ohne Speicherung
5 zwischen den Betriebszyklen des Steuergeräts und ohne externe Quellen (zufällige Trigger) erzeugt werden können.

Diese Aufgabe wird durch die Merkmale der unabhängigen Ansprüche gelöst.

10

Vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

15

Das erfindungsgemäße Verfahren baut auf dem gattungsgemäßen Stand der Technik dadurch auf, dass die echte Zufallszahl auf der Grundlage einer stochastisch verteilten Dauer eines elektrischen Umladevorgangs erzeugt wird. Durch diese Lösung wird eine echte Zufallszahl erzeugt, das heißt keine Pseudo-Zufallszahl. Weiterhin kann das Verfahren nicht durch externe

20

Beschaltung manipuliert werden. In vielen Fällen werden gegenüber der vorhandenen Bestückung des jeweiligen Systems keine weiteren Bauteile benötigt, so dass die Zusatzkosten gering sind. Ein weiterer Vorteil des erfindungsgemäßen Verfahrens besteht darin, dass es nicht erforderlich ist, einen

25

Zustand zu speichern, der dann manipuliert beziehungsweise zurückgesetzt werden könnte. Das erfindungsgemäße Verfahren ist besonders vorteilhaft, wenn der die stochastische Quelle bildende Umladevorgang in einer Komponente durchgeführt werden kann, die ohnehin Bestandteil des Systems ist, das neben
30 der Erfüllung anderer Aufgaben auch die Zufallszahl erzeugen muss.

Bei bevorzugten Ausführungsformen des erfindungsgemäßen Verfahrens ist vorgesehen, dass der Umladevorgang ein Umladen zumindest einer Speicherzelle umfasst. Speicherzellen sind ohnehin Bestandteil moderner Systeme und stellen daher eine
5 besonders kostengünstige Grundlage zur Durchführung des Umladevorgangs dar.

In diesem Zusammenhang kann beispielsweise vorgesehen sein, dass zumindest eine Speicherzelle eine Speicherzelle eines
10 EEPROM ist. Die Dauer eines Umladevorgangs einer EEPROM-Speicherzelle unterliegt vergleichsweise großen stochastischen Streuungen, auf deren Grundlage sich echte Zufallszahlen erzeugen lassen.

15 Alternativ ist es ebenfalls möglich, dass zumindest eine Speicherzelle eine Speicherzelle eines FLASH-Speichers ist. FLASH-Speicher finden zunehmend Verwendung und stellen daher in vielen Fällen ohne zusätzliche Kosten eine geeignete Grundlage für die erfindungsgemäße Erzeugung von echten Zu-
20 fallszahlen dar.

Bei bevorzugten Ausführungsformen des erfindungsgemäßen Verfahrens ist weiterhin vorgesehen, dass der Umladevorgang mit Hilfe einer Ladungspumpe durchgeführt wird. Der Einsatz von
25 Ladungspumpen ist beispielsweise im Zusammenhang mit EEPROMs üblich, wobei in vielen Fällen On-Chip-Ladungspumpen vorgesehen sind.

Bei dem erfindungsgemäßen Verfahren kann in vorteilhafter
30 Weise weiterhin vorgesehen sein, dass die stochastische Dauer des Umladevorgangs mit Hilfe eines Zählers erfasst wird. Dabei ist es vorteilhaft, wenn die Taktung des Zählers möglichst hoch ist, so dass sich hinsichtlich des als Grundlage

für die Zufallszahl dienenden Zählerstandes am Ende des Umladevorgangs möglichst große Streuungen ergeben.

Das erfindungsgemäße Verfahren wird als besonders vorteilhaft
5 erachtet, wenn vorgesehen ist, dass es von einem Embedded-System durchgeführt wird, insbesondere von einer Motorsteuerung eines Kraftfahrzeugs. Dabei kommen prinzipiell alle Embedded-Systems in Frage, die in Umgebungen eingesetzt werden, in denen (auch) die Erzeugung von guten Zufallszahlen erforderlichlich ist.
10

Die erfindungsgemäße Vorrichtung baut auf dem gattungsgemäßen Stand der Technik dadurch auf, dass sie die echte Zufallszahl auf der Grundlage einer stochastisch verteilten Dauer eines
15 elektrischen Umladevorgangs erzeugt. Dadurch ergeben sich die im Zusammenhang mit dem erfindungsgemäßen Verfahren erläuterten Vorteile und Eigenschaften in gleicher oder ähnlicher Weise, weshalb zur Vermeidung von Wiederholungen auf die entsprechenden obigen Ausführungen verwiesen wird.
20

Gleiches gilt sinngemäß für die nachfolgend angegebenen vorteilhaften Weiterbildungen der erfindungsgemäßen Vorrichtung, wobei auch diesbezüglich auf die entsprechenden Ausführungen im Zusammenhang mit dem erfindungsgemäßen Verfahren verwiesen
25 wird.

Die erfindungsgemäße Vorrichtung ist in vorteilhafter Weise dadurch weitergebildet, dass sie zumindest eine Speicherzelle aufweist, die zur Erzeugung der Zufallszahl elektrisch umge-
30 laden wird.

Dabei kann in vorteilhafter Weise vorgesehen sein, dass zumindest eine Speicherzelle eine Speicherzelle eines EEPROM ist.

- 5 Zusätzlich oder alternativ ist es möglich, dass zumindest eine Speicherzelle eine Speicherzelle eines FLASH-Speichers ist.

10 Die erfindungsgemäße Vorrichtung ist in vorteilhafter Weise dadurch weitergebildet, dass sie zur Durchführung des Umladevorgangs eine Ladungspumpe aufweist.

15 Im Zusammenhang mit der erfindungsgemäßen Vorrichtung kann weiterhin vorgesehen sein, dass sie zur Erfassung der stochastisch verteilten Dauer des Umladevorgangs einen Zähler aufweist.


20 Als besonders vorteilhaft werden Ausführungsformen der erfindungsgemäßen Vorrichtung erachtet, bei denen vorgesehen ist, dass sie ein Embedded-System ist, insbesondere eine Motorsteuerung eines Kraftfahrzeugs.

25 Ein wesentlicher Grundgedanke der vorliegenden Erfindung besteht darin, dass echte Zufallszahlen praktisch ohne Mehrkosten von Systemen erzeugt werden können, wenn als stochastische Quelle eine ohnehin zum System zählende Komponente verwendet wird, beispielsweise eine Ladungspumpe, die Bestandteil eines Steuergeräts ist. Die Erfindung eignet sich insbesondere für alle Dienststellen, die mit vorhandenen Systemen
30 (das heißt ohne extra dafür vorgesehene Bauteile) eine gute, echte Zufallszahl erzeugen müssen, ohne Zugriff auf unabhängige, manipulationssichere Generatoren (Trigger) zu haben. Darunter fallen, ohne darauf beschränkt zu sein, insbesondere

alle kostenoptimierten Embedded-Systems. Im Zusammenhang mit der Kraftfahrzeugtechnik werden Zufallszahlen beispielsweise insbesondere für den Zugriffsschutz (auch bei Wartungsarbeiten) und für Verschlüsselungszwecke (zum Beispiel Wegfahr-
 5 sperre) benötigt.

Ausführungsformen der Erfindung werden nachfolgend anhand der zugehörigen Zeichnungen beispielhaft erläutert.


10 Es zeigen:

 Figur 1 ein Flussdiagramm, das eine Ausführungsform des erfindungsgemäßen Verfahrens veranschaulicht;

15 Figur 2 einen Graph, der mögliche Umladevorgänge einer Speicherzelle veranschaulicht;

Figur 3 ein stark vereinfachtes, schematisches Blockschaltbild von Komponenten einer Motorsteuerung.

20

 Die in Figur 1 dargestellte Ausführungsform des erfindungsgemäßen Verfahrens beginnt beim Schritt S1. Im Schritt S2 wird ein Zähler zurückgesetzt, dessen späterer Zählerstand als Grundlage für die Erzeugung der echten Zufallszahl dient oder
 25 der diese Zufallszahl direkt darstellt. Im Schritt S3 wird ein Umladevorgang begonnen und gleichzeitig der Zähler gestartet. Bei dem Umladevorgang kann es sich insbesondere um ein Schreiben in eine EEPROM- oder FLASH-Speicherzelle handeln, das üblicherweise unter Verwendung einer Ladungspumpe
 30 erfolgt. Im Schritt S4 wird solange geprüft, ob der Umladevorgang abgeschlossen ist, bis dies der Fall ist. Anschließend wird im Schritt S5 der Zähler gestoppt. Im Schritt S6 wird der Zählerstand ausgelesen und als echte Zufallszahl

verwendet. Gegebenenfalls kann die endgültige Zufallszahl jedoch auch unter Zuhilfenahme weiterer Rechenfunktion erzeugt werden. Das dargestellte Verfahren endet im Schritt S7.

- 5 Figur 2 veranschaulicht drei stochastisch verteilte Umladevorgänge einer Speicherzelle. Die tatsächliche Dauer eines aktuellen Umladevorgangs kann dabei zwischen einer kürzesten Dauer T' (Kurve Q') und einer längsten Dauer T'' (Kurve Q'') liegen und beispielsweise T (Kurve Q) betragen.

10

Figur 3 zeigt ein stark vereinfachtes, schematisches Blockschaltbild von Komponenten einer Motorsteuerung, wobei die dargestellte Motorsteuerung 18 in Form eines Embedded-Systems vorliegt. Die Motorsteuerung 18 kann eine Vielzahl weiterer nicht dargestellter Komponenten umfassen, die zur Erfüllung aller an die Motorsteuerung gestellten Aufgaben erforderlich sind. Sämtliche im Folgenden näher erläuterten Komponenten sind ohnehin Bestandteil der Motorsteuerung 18, das heißt nicht speziell zur Erzeugung der echten Zufallszahlen vorgesehen. Die dargestellte Motorsteuerung 18 weist einen intelligenten Controller 20 auf, der unter anderem dazu geeignet ist, eine Ladungspumpe 14 anzusteuern, die dazu vorgesehen ist, eine Speicherzelle 10 eines Speicherzellenarrays 22 eines EEPROMs 12 umzuladen, wenn der Inhalt der Speicherzelle 10 verändert werden soll. Der Controller 20 kommuniziert weiterhin mit einem Zähler 16, mit dem die tatsächliche Dauer eines Umladevorgangs der Speicherzelle 10 erfasst wird. Der Fachmann erkennt, dass mit den in Figur 3 dargestellten Komponenten das anhand von Figur 1 erläuterte Verfahren in vorteilhafter Weise durchgeführt werden kann. Auf eine erneute Erläuterung des Ablaufs der Erzeugung einer Zufallszahl wird daher an dieser Stelle verzichtet.

Die in der vorstehenden Beschreibung, in den Zeichnungen sowie in den Ansprüchen offenbarten Merkmale der Erfindung können sowohl einzeln als auch in beliebiger Kombination für die Verwirklichung der Erfindung wesentlich sein.

Patentansprüche

1. Verfahren zum Erzeugen einer echten Zufallszahl,
dadurch gekennzeichnet,
5 dass die echte Zufallszahl auf der Grundlage einer stochastisch verteilten Dauer (T) eines elektrischen Umladevorgangs erzeugt wird.
2. Verfahren nach Anspruch 1,
10 dadurch gekennzeichnet,
dass der Umladevorgang ein Umladen zumindest einer Speicherzelle (10) umfasst.
3. Verfahren nach Anspruch 2,
15 dadurch gekennzeichnet,
dass zumindest eine Speicherzelle (10) eine Speicherzelle eines EEPROM (12) ist.
4. Verfahren nach Anspruch 2 oder 3,
20 dadurch gekennzeichnet,
dass zumindest eine Speicherzelle (10) eine Speicherzelle eines FLASH-Speichers ist.
5. Verfahren nach einem der vorangehenden Ansprüche,
25 dadurch gekennzeichnet,
dass der Umladevorgang mit Hilfe einer Ladungspumpe (14) durchgeführt wird.
6. Verfahren nach einem der vorangehenden Ansprüche,
30 dadurch gekennzeichnet,
dass die stochastische Dauer (T) des Umladevorgangs mit Hilfe eines Zählers (16) erfasst wird.

7. Verfahren nach einem der vorangehenden Ansprüche,
dadurch gekennzeichnet,
dass es von einem Embedded-System (18) durchgeführt wird,
insbesondere von einer Motorsteuerung (18) eines Kraftfahr-
5 zeugs.

8. Vorrichtung, die zur Erzeugung einer echten Zufallszahl
geeignet ist,
dadurch gekennzeichnet,
10 dass sie die echte Zufallszahl auf der Grundlage einer sto-
chastisch verteilten Dauer (T) eines elektrischen Umladevor-
gangs erzeugt.

9. Vorrichtung nach Anspruch 8,
15 dadurch gekennzeichnet,
dass sie zumindest eine Speicherzelle (10) aufweist, die zur
Erzeugung der Zufallszahl elektrisch umgeladen wird.

10. Vorrichtung nach Anspruch 9,
20 dadurch gekennzeichnet,
dass zumindest eine Speicherzelle (10) eine Speicherzelle ei-
nes EEPROM (12) ist.

11. Vorrichtung nach Anspruch 9 oder 10,
25 dadurch gekennzeichnet,
dass zumindest eine Speicherzelle (10) eine Speicherzelle ei-
nes FLASH-Speichers ist.

12. Vorrichtung nach einem der Ansprüche 8 bis 11,
30 dadurch gekennzeichnet,
dass sie zur Durchführung des Umladevorgangs eine Ladungspum-
pe (14) aufweist.

13. Vorrichtung nach einem der Ansprüche 8 bis 12,
dadurch gekennzeichnet,
dass sie zur Erfassung der stochastisch verteilten Dauer (T)
des Umladevorgangs einen Zähler (16) aufweist.

5

14. Vorrichtung nach einem der Ansprüche 8 bis 13,
dadurch gekennzeichnet,
dass sie ein Embedded-System (18) ist, insbesondere eine Mo-
torsteuerung (18) eines Kraftfahrzeugs.

10



Zusammenfassung

Manipulationssichere Erzeugung von echten Zufallszahlen

- 5 Die Erfindung betrifft ein Verfahren und eine Vorrichtung zum Erzeugen einer echten Zufallszahl.

Erfindungsgemäß ist vorgesehen, dass die echte Zufallszahl auf der Grundlage einer stochastisch verteilten Dauer (T) eines elektrischen Umladevorgangs erzeugt wird. Dabei kommen
10 insbesondere Umladevorgänge von Speicherzellen, beispielsweise EEPROM- oder FLASH-Speicherzellen, in Betracht, die mit Hilfe einer Ladungspumpe durchgeführt werden.

15 Figur 2

113

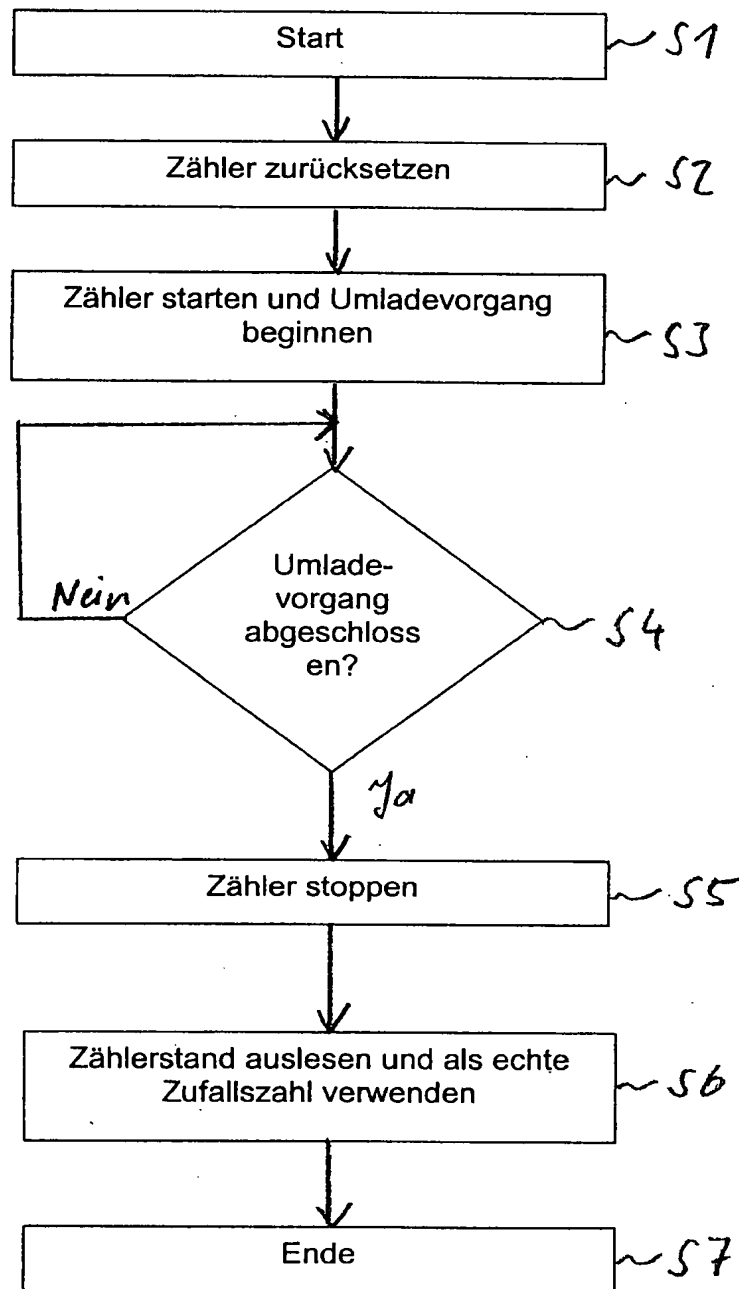


Fig. 1

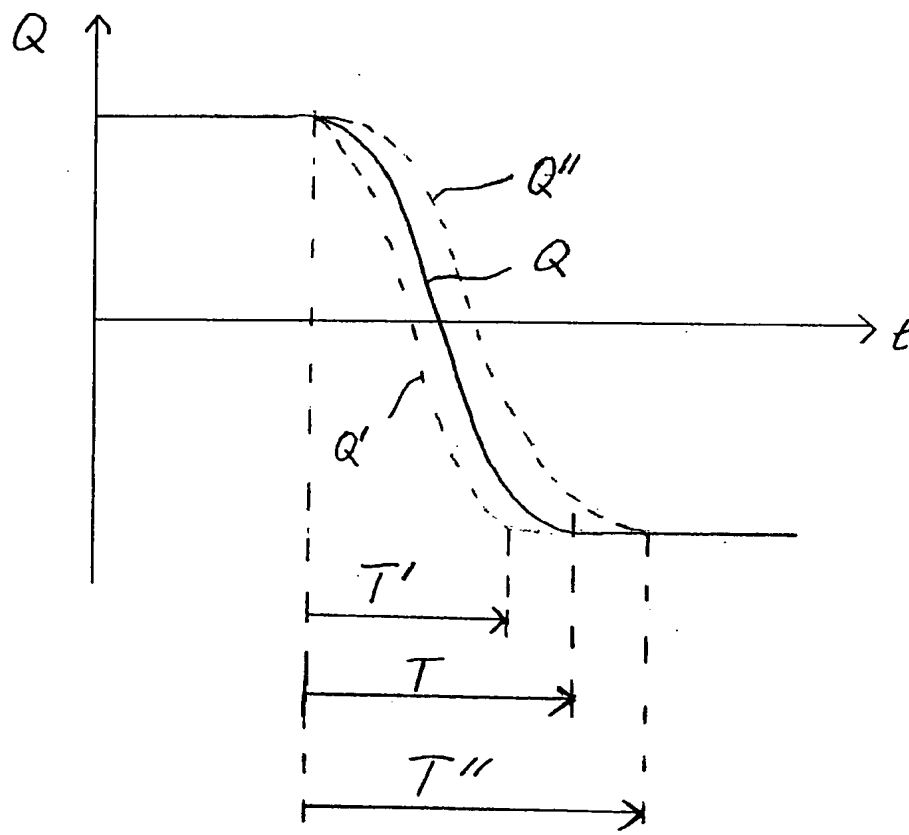


Fig. 2

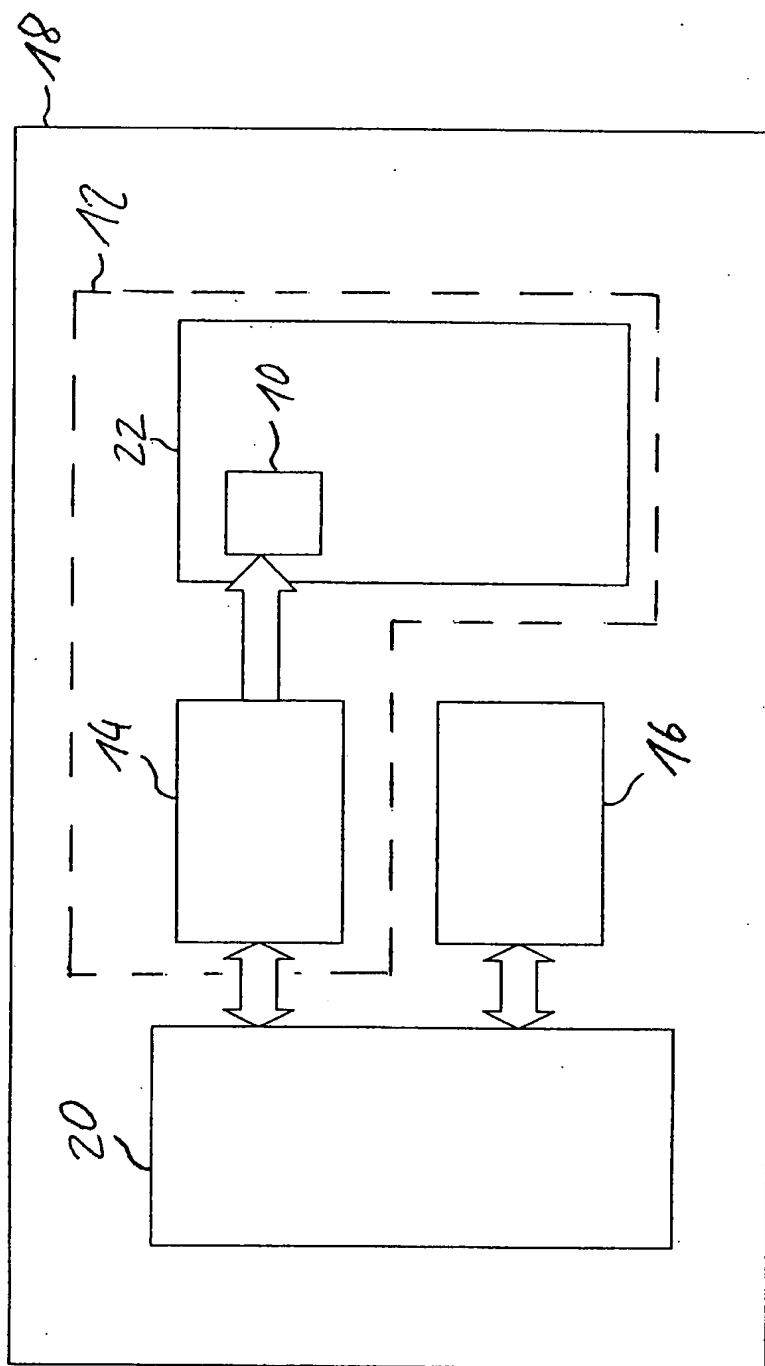


Fig. 3